3e Technologies International, Inc.
FIPS 140-2
Non-Proprietary Security Policy

3e-010f Cryptographic Client Software
(Version 2.0)

December 02, 2003

TABLE OF CONTENTS

Glossary of terms

FIPS	Federal Information Processing Standard
DMG	Dual Mode Gateway
LAN	Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
SHA	Secure Hash Algorithm
RSA	Rivest, Shamir, Adleman
DHCP	Dynamic Host Configuration Protocol
TLS	Transport Layer Security
CSP	Critical Security Parameter
CO	Cryptographic Officer
EAP	Extensible Authentication Protocol
AP	Access Point
PRNG	Pseudo Random Number Generator
EAP	Extensible Authentication Protocol
SRDI	Security Relevant Data Item
MAC	Medium Access Control
SSID	Service Set Identifier
GUI	Graphical User Interface
SRDI	Security Relevant Data Item

1. Introduction

1.1 Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International, Inc.'s 3e-010f Cryptographic Client Software (Version 2.0); hereafter know as the Crypto Client. This software is intended to run on Windows Based Client devices such as laptop computers, PDAs, Network Capable Application Processors(NCAP), other embedded devices running the Windows. This software was created to communicate with the 3eTI Family of Wireless Gateways which are designed and manufactured by 3eTI. This policy was created to satisfy the requirements of FIPS 140-2 Level 1. This document defines 3eTI's security policy and explains how Crypto Client software meets the Level 1 FIPS 140-2 requirements.

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules* available on the NIST website at http://csrc.nist.gov/cryptval/.

1.1. Definition

The Crypto Client is a set of software components and utilities. This includes a wireless card driver that does packet-level encryption/decryption, a GUI-based configuration utility and a service that does dynamic key exchange. The Crypto Client operates in one of three modes, Bypass, AES Encryption and 3DES Encryption. The cryptographic boundary of the Crypto Client is defined as in Figure 1. Crypto Client is software running on a laptop within a Windows Operating Environment. The module can be run on Windows NT 4.0 (Service Pack 6), Windows 2000 or Windows XP. The Operating System must be configured to run single-user mode (See Section 3). For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product.

3eTI client software provides the following major services:

- The Crypto Client Software provides encryption/decryption (AES/3DES) for secure wireless communication with a 3eTIGateway. It restricts the unauthorized access to data transferred across the wireless network. The 802.1b wireless signals are transmitted by the driver in encrypted form using AES/3DES. All incoming packets must also be encrypted unless the module is in bypass mode.
- The Crypto Client Software provides dynamic session key exchange for wireless communication. It reduces the security threat for unauthorized users to break the cryptographic key for the wireless network. This is based on the EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) open system authentication.

- The 3eTI client provides a password-based authentication to the configuration utility. The CO and Admin must login before any configuration changes are made on the client.
- The client provides secure storage of cryptographic keys and passwords in the Windows registry.

1.2. Scope

This document will cover the secure operation of the 3e-010f Crypto Client including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

2. Roles, Services, and Authentication

The 3eTI Crypto Client supports four separate roles. The set of services available to each role and corresponding authentication mechanisms are defined in this section.

2.1 Roles and Services

2.1.1. Services

The 3eTI Crypto Client provides the following major services:

- Wireless 802.11b secure communication with a 3eTI Wireless Access Point (AP).
- Wireless Site Survey to obtain a list of all Gateways in the vicinity of the client
- Wireless Signal Strength Settings
- Wireless Transmit Rate Control
- Configure Profiles, Delete Profiles (SSID, Encryption Type, Static keys)

The 3eTI Crypto Client provides the following FIPS-Approved cryptographic algorithms:

- AES ECB for encryption/decryption of 802.11b wireless packets. All keysizes (128, 192, 256-bit) are supported
- 3DES ECB for encryption/decryption of 802.11b wireless packets (192-bit keysize)
- 3DES CBC for encrypting RSA private key (192-bit keysize).
- SHA-1 hashing for EAP-TLS protocol.
- HMAC-SHA1 for software integrity check.
- RSA PKCS#1 Signature Generation to sign messages during EAP-TLS session.
- The client uses an Approved RNG as per FIPS 186-2 Appendix 3 (3.1, 3.2, and 3.3).

The module supports the EAP-TLS protocol for authentication of the client to the Gateway and for negotiating the TLS session key that becomes the unicast key for that session.

The Crypto Client also supports non-Approved RSA Encryption using the public key. The module uses RSA Encryption in a FIPS-compliant manner for key transport.

2.1.2. Roles

The 3eTI Security client supports the following authorized roles for operators:

Crypto Officer Role: The Crypto Officer role performs all security functions provided by the Crypto Client using the GUI-based configuration utility. This role performs cryptographic initialization, configuration and management functions (e.g., module initialization and configuration, configuring encryption mode, input/output of cryptographic keys and CSPs, and audit functions). The Crypto officer must operate within the Security Rules specified in Section 3.1. The Crypto officer must also ensure that the module is in FIPS mode of operation by following the steps outlined in Section 3.2. Only one Crypto Officer is defined in the client. The Crypto Officer authenticates to the client using a username and password.

Administrator Role: The Administrator role is considered the User role for FIPS purposes. The Administrator can send and receive plaintext (in BYPASS mode) and encrypted wireless data packets (in encryption mode). The Administrator can also monitor the configuration settings and perform self-tests using the GUI-based configuration utility. The Administrator can view the system log and application messages using the Windows Event Viewer for auditing purposes. No keys or CSPs are accessible to the Administrator. The Administrator does not have any privileges to modify configuration settings. The Administrator Role is authenticated using username and password. Only a single Administrator role exists

The following table lists the services provided to the CO and Administrator

Role	**Authorized Services**
Administrator and Crypto Officer	TX Power Mode Setting
	Launch GUI Self Test
	Disable Radio
	Reset Radio
	View encryption mode and configuration settings
	View signal strength, link quality, transmission rate and channel number
	View Event viewer
	Encryption/decryption of wireless data
	Bypass service
	Key zeroization
Crypto Officer Only	Profile Creation and Deletion
	SSID Setting
	Restore Crypto Client to factory defaults
	Enter static encryption keys
	View system processes
	Set Transmit Rate
	Encryption Type Selection:

	- None/Bypass - Static AES (128-bit, 192-bit, 256-bit) - Static 3DES - Dynamic
	For Dynamic Key Exchange enter - Certificate file - Private key file - Private key password - View client authentication status

Security Server Role: This role is assumed by the authentication server, which is a self-contained workstation connected to the 3eTI Wireless Gateway over the Ethernet Uplink WAN port. The Security Server is employed for authentication of the client to the Gateway and key management activities. Only one Security Server is supported.

The Security Server is used only during dynamic key exchange. The Security Server establishes an EAP-TLS session with the client to negotiate the TLS session key (unicast key) with the client during dynamic key exchange. No authentication is required by the client for the Security Server. However, the Security Server authenticates to the Gateway using a shared-secret.

Gateway Role: This role is assumed by the FIPS 140-2 validated 3eTI Wireless Gateway that uses static or dynamic key AES or 3DES encryption to communicate wirelessly with the client. The wireless Gateway acts as an access point providing a communication link from the wireless Crypto Client to the wired uplink LAN and the wireless LAN. Details of the 3eTI Gateway device are contained in the 3e-DMG security policy. The Gateway acts as a User role for FIPS purposes

3eTI Crypto Client operates in an infrastructure network mode, so every Crypto Client must communicate directly with a 3eTI Gateway device acting in the Gateway Role. The Gateway sends encrypted packets received from other workstations to the client using the current encryption mode and keys. All packets transmitted by the client are sent to the Gateway who then routes the packets to the appropriate destination. No authentication is required by the client for the Gateway. The Crypto Officer must configure the Gateway SSID on the client in order to allow the Gateway to communicate with the client. The client can only communicate with one Gateway at any given time. However, upto 4 Gateway SSIDs can be configured on the client.

The services provided by the client to the Gateway include:

- Use static or dynamic key AES or 3DES encryption to communicate wirelessly with the client
- Dynamic session key exchange (Diffie-Hellman modulo 1024) for wireless communication.
- BYPASS mode of operation in which wireless packets are exchanged in plaintext.

2.2 Authentication Mechanisms and Strength

The following table summarizes the four roles and the type of authentication supported for each role:

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-Based	Username and password
Administrator	Role-Based	Username and password
Security Server	None	None
Gateway	None	None

The following table identifies the strength of authentication for each authentication mechanism supported:

Authentication Mechanism	Strength of Mechanism
Password	Minimum 6 characters => 72^6 = 1.39E11

3 Secure Operation and Security Rules

3.1 Security Rules

The following security rules must be followed by the operator in order to ensure secure operation:

1. Every user (Crypto Officer or Administrator) has a username on the Crypto Client. No user will violate trust by sharing his/her password associated with the username with any other user or entity.
2. The Crypto Officer will not share any key, CSP, or SRDI used by the Crypto Client with any other user or entity.
3. The user will explicitly logoff by closing the configuration utility each time.
4. The Administrator and Crypto officer will monitor the Windows application log using the Control Panel -> Administrative Tools -> Event Viewer program periodically for self-test errors. All status indicators in case of self-test errors are logged in the Event Viewer. The Administrator and CryptoOfficer will also ensure that WinSupp service is running each time the workstation is re-booted or the driver is reset.

3.2 FIPS mode of operation

The following steps must be performed to install and initialize the module for operating in a FIPS 140-2 compliant manner:
1. The operating system must be configured to prevent remote login and access to the workstation as a server. The operating system must be configured to run in single-user mode. For Windows NT/2000/XP, this can be done by disabling the Server and RunAsService services using the Control Panel Services program.

2. The paging file (Virtual memory) must be configured to reside on a local drive on the workstation, not a network drive.
3. The operator must verify that the WinSupp service is always running in order for the module to be in FIPS mode of operation. This can be done by using the Services program in Control Panel. The WinSupp service should be configured as having Automatic startup. If the Services settings are not modified after installation this should always be the case.

3.3 FIPS Policy

The following policies must always be followed in order to achieve a FIPS 140-2 mode of operation:
1. The cryptographic module must only be used by one human operator at a time, and must not be actively shared among operators at any time.
2. None of the files belonging to the module that are installed on the machine should be moved from their original location.
3. The 3eTI client Administrator (end-user of the laptop) must not be given Windows Administrative privileges on the workstation. This will prevent the Administrator from modifying any registry key values, disabling WinSupp service or uninstalling the 3eTI client software using the Control Panel Add/Remove Programs applet.
4. The 3eTI client Crypto Officer must have Administrative privileges on the workstation on which the module is run. This will allow the CO to install the software and wireless driver and uninstall the software if needed.

3.4 Secure Operation Initialization

3.4.1 Installing the advanced encryption driver

The 3e-010f Crypto Client driver needs to be installed on each wireless device that needs to access the WLAN. 3e Technologies International's wireless driver is compatible with wireless cards based on INTERSIL PRISM 2 and 2.5 chipsets like Samsung, CC&C, and Senao. It should be installed in a Windows 2000, Windows NT 4.0 or Windows XP operating system environment.

Before installation

Important Note: If the manufacturer's wireless card utility for the PC card has been previously installed, it needs to be uninstalled before installing the 3e encryption utility.

For many PC Cards, there will be an uninstall command on the Start -> Programs menu under the wireless card's utility. If this is not an option on the laptop, the operator can, instead, uninstall using Windows **Add/Remove Programs** utility. To do this, double-click **My Computer** and double-click the **Control Panel** to open its window. The operator will find an icon for Add/ Remove Programs. Double-click the icon to open the **Add/Remove Programs** window, and locate the manufacturer's software. Click the **Change/Remove** button.

Answer **Yes** to the following pop-up screen. Windows will remove the software from your computer and show what it is doing. Once this is complete, the operator can install the 3e Technologies International drivers.

Installing the driver

Note: It is recommended that the operator close all open Windows programs before beginning the install Wizard. Also take the wireless PC Card out of the PC Card slot.

Insert the 3e-010f Crypto Client Install CD in the CD-ROM drive. The CD should autoplay and display a menu that will allow you to start the install process using a typical installation program

NOTE: If the laptop has autoplay set off, from **My Computer**, locate the CD-Rom drive symbol and double-click to open its window. Locate the **autoplay.exe** file and double click to bring up the menu. Or, find the setup.exe file and click to begin the installation process immediately. The InstallShield Wizard guides the operator through the install process. First, the following introductory splash screen is seen

The Wizard will begin the install process, as shown on the next screen. Click **Next** to continue.

The operator needs to read and accept the terms of the 3eTI license agreement before the install can continue.

On the next screen, the operator can confirm the default Destination location or select an alternate folder where the setup procedure will place the files.

On the following screen, the operator is given the opportunity to cancel or go back to make changes. Once you click the Install button, the Wizard will begin the installation.

Once the installation Wizard says the installation is complete, click **Finish**. Then, put the wireless PC card back in the slot. Windows will find new hardware.

The operator may see the Windows Digital Signature screen at this point. Click **Yes** and continue.

Once the driver utility has been installed, a tiny PC card icon will appear on the taskbar at the bottom right side of the desktop whenever your PC card is in its slot. The icon will have a red X across it if the client is not associated or if there are any errors.

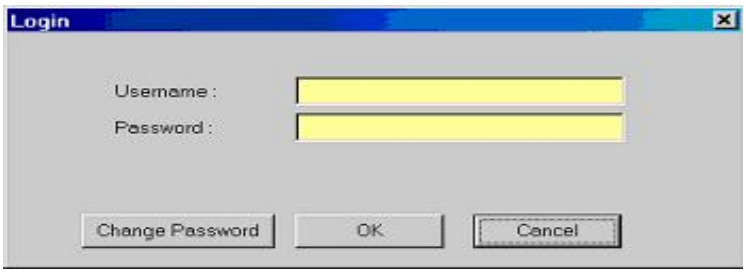
The operator should now configure the encryption utility to allow access to the WLAN. Until the utility has been configured to allow access to the gateway, the wireless device will not be able to access the WLAN.

3.4.2 Configuring the encryption utility on the client device

The operator open the utility by using Start -> Programs -> 3e-010F Crypto Client Software -> Config Utility.

On the other hand, the operator can double-click the icon on the taskbar to bring up the 3e-010f Crypto Client Wireless Settings utility.

Login



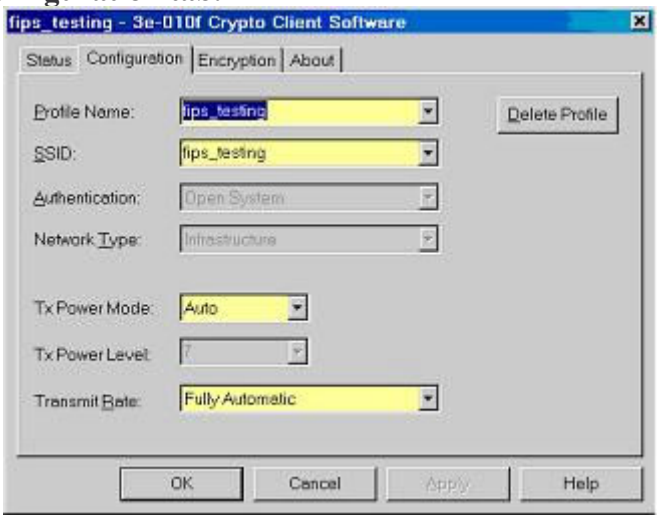
The Driver configuration utility requires login. This is to safeguard the device to make sure no malicious use of the wireless card.

The Username cannot be changed. The password can be changed. Press the **Change Password** button and the following screen will show up:

Type the correct **Old Password** and **New Password** and press **OK** to change the password. The password length has to be at least 6 characters.

Until configuration is complete, no information as to status will show on the **Status** tab. Each tab, however, has a Help button with useful information.

Tab first to the Configuration tab.



Select a **Profile Name** that will be used to identify which WLAN the device is going to be accessing. This is an arbitrary name. Multiple profiles can set up if the operator will be using the laptop on different WLANs at different times. Each will have its own separate

set of parameters. If the CO sets up a Profile name that he/she later wants to delete, simply use the **Delete Profile** button with the name of the profile that is to be deleted showing. A **Delete Wireless Profile** window will ask the CO to confirm the decision.

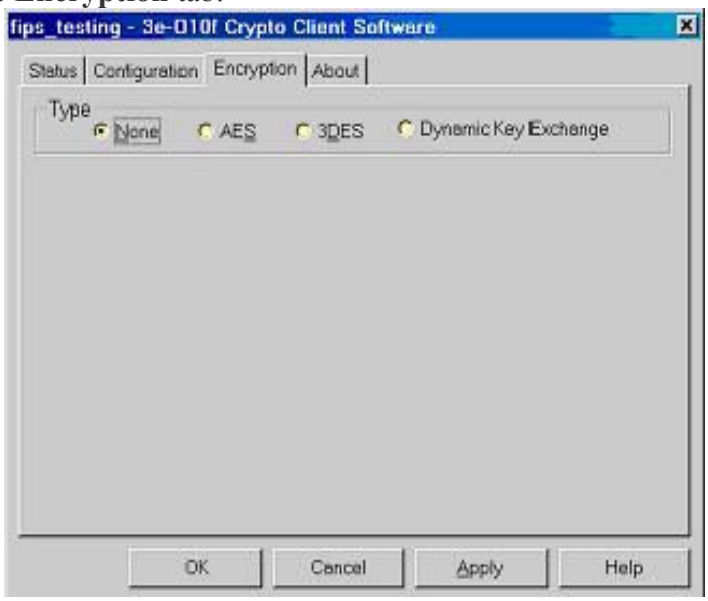
In the **SSID** dropdown menu on the Configuration tab, input the exact **SSID** of the WLAN. The SSID acts as the basic password/identification for the WLAN and must be the same for each wireless device as for the access point. An SSID is case sensitive. That is, the case (upper or lower) of each of the letters used in the SSID must be the same on the laptop and access point.

Authentication and **Network Type** are grayed out in FIPS mode. Authentication is always open system. Network Type is always "Infrastructure", which means the device always talks to an AP/Gateway.

Tx Power Mode can be set to either **Auto** or **Fixed**. **Auto** is the default value and is recommended for most users. If an operator needs to lower the transmission power for some reason, the **Tx Power Mode** can be set to **Fixed** and the **Tx Power Level** can be adjusted. The bigger the number, the higher the transmitting power.

Transmit Rate probably should be left, in most instances, in the default value of "Fully Automatic." The **Defaults** button, if selected, sets all values back to factory default.

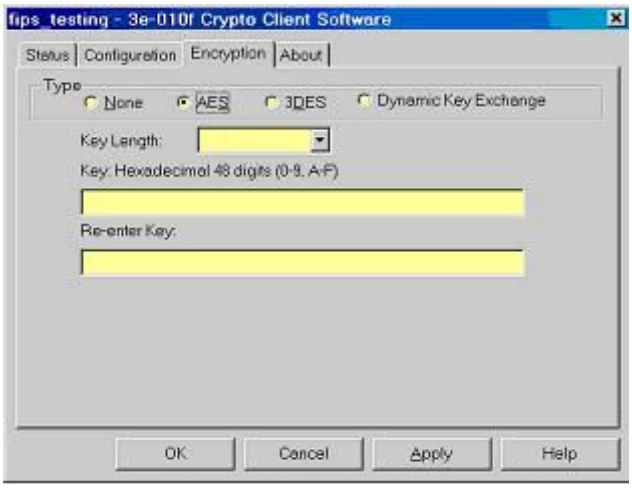
Next, click on the **Encryption** tab.



The default encryption type is none.

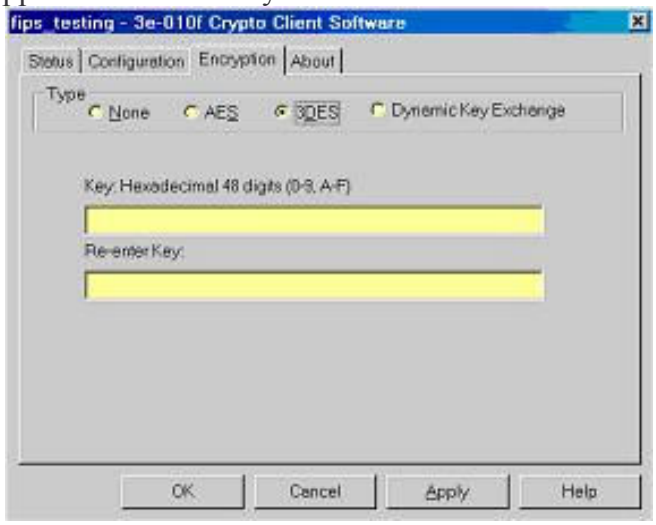
Important Note: When encryption of any kind is being used, there will be some decrease in throughput. This is due to the application of the encryption algorithm and the operating environment.

If the CO chooses the radio button for **AES** encryption on the encryption tab, the menu shown next will appear.



In the **Key Length** block, the CO can specify 128-bit, 192-bit, or 256-bit key length. Select the appropriate one for the configuration and type the key value in Hex in the following block.

If the CO chooses the radio button for **3DES** encryption on the encryption tab, the menu shown below will appear. The 3DES key will be 48 hexadecimal characters long.



If the CO chooses the radio button for **Dynamic Key Exchange** encryption on the encryption tab, the menu shown below will appear.

In **Certificate,** specify the location of the X509 certificate. The format should be **DER** format. In **Key**, specify the location of the private key file that corresponds to the certificate. The key should be in **PEM** format. In **CA**, point to the certificate file of the CA, which signed the certificate. In **Password**, put the secret being used to protect the private key.

Once the CO clicks **Apply**, the dynamic key exchange is initiated and the **status bar** shows whether the authentication with the **Security Server** through the **AP/Gateway** is successful or not.

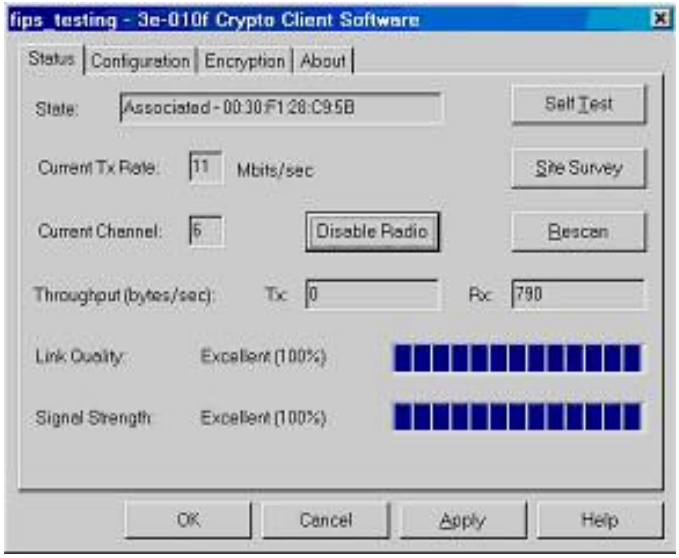
NOTE: The **AP** and **Security Server** must be configured properly before the authentication succeeds. Also the CO must input the correct **SSID** in the **Configuration** tab.

Once the CO has established the specific parameters for communicating with the WLAN, the CO must click **Apply** to save all parameters.

3.4.3 Verify the Status

Close all windows and double-click the card utility icon on the taskbar. (The operator can also access the configuration utility by selecting it from Start -> Programs -> 3e-010F Crypto Client Software or by selecting the 3e-010f icon from the Control Panel.)

When the utility window appears, select the **Status** tab. The operator should now see the status of the association to the wireless gateway/AP. In the **State** section, the MAC address of the AP that is handling communication from the device that is configured should appear. The operator can monitor the transfer rate and observe the channel and throughput.



To see all the APs currently configured in the LAN, push the **Site Survey** button. This initiates a non-destructive scan and displays a list of all access points detected.

To the left of the **Rescan** button is a Disable/Enable Radio toggle. This toggle button can be used if there is a need to take the client machine off of the radio transmission frequency.

To stop the card from transmitting temporarily, select the **Disable Radio** button. The card state will change to **Radio Off**. The card can be put back into normal operation by selecting the **Enable Radio** button.

On the **Status** tab, the operator can also reset the card by using the **Rescan** button. Selecting **Rescan** issues a software reset to the driver software and the card will try to associate with the access point again.

The **Status** screen also indicates **Link Quality** and **Signal Strength** after the client has associated with the access point.

The utility also includes an **About** tab. This tab simply shows version number and other general information.

From the version number, an operator can tell whether there is a need to install an available update to the software. The entire software package needs to be reinstalled which will overwrite the existing installation.

4. Physical Security

The Crypto Client is a set of software components that have been tested on the Windows NT 4.0 (Service Pack 6), Windows 2000 and Windows XP configured for single-user mode. It can be run on other Windows Operating Systems but was not tested on these platforms. The Crypto Client was tested on Standard Intel Personal Computer Platforms (PC) and 3e-TI Network Capable Application Processor Platform (NCAP) and meets all FIPS 140-2 Level 1 physical security requirements. The module itself does not provide any physical security mechanisms.

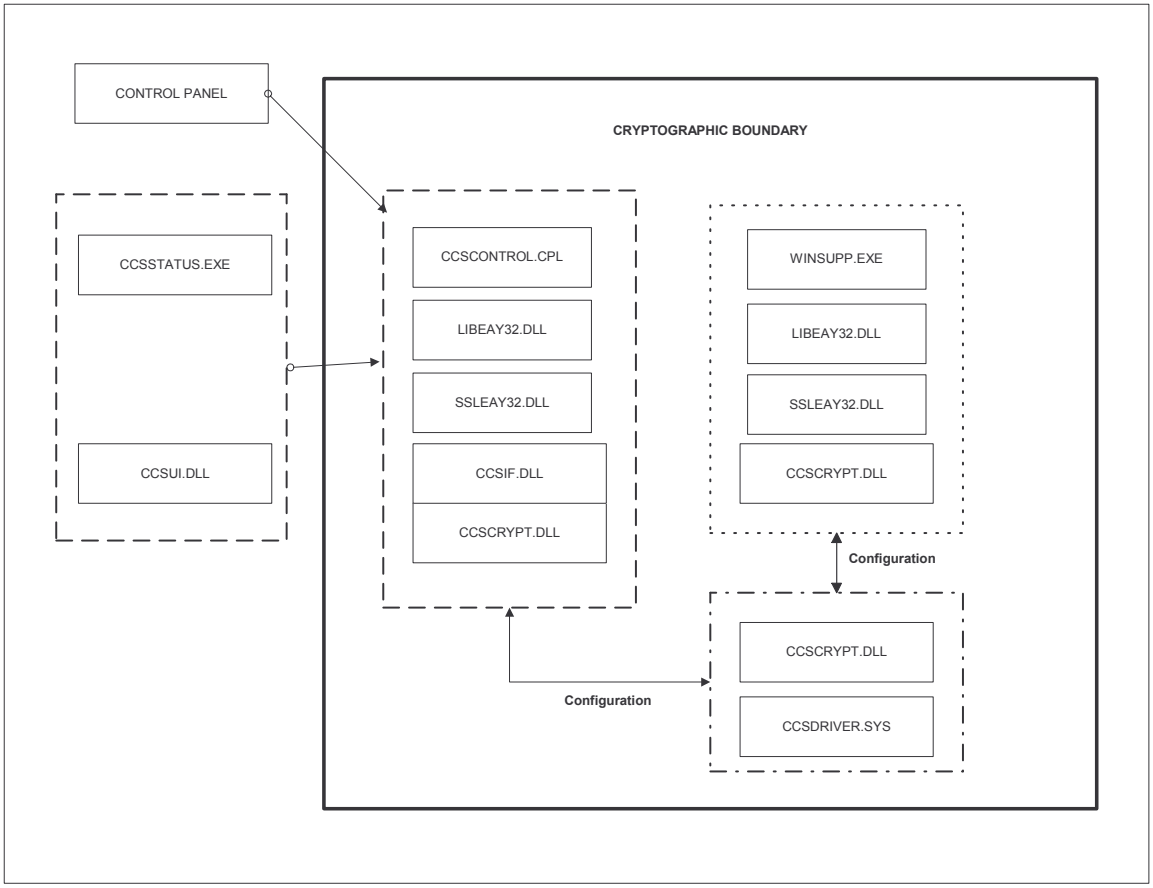

CONTROL PANEL
CRYPTOGRAPHIC BOUNDARY
CCSSTATUS.EXE
CCSUI.DLL
CCSCONTROL.CPL
LIBEAY32.DLL
SSLEAY32.DLL
CCSIF.DLL
CCSCRYPT.DLL
WINSUPP.EXE
LIBEAY32.DLL
SSLEAY32.DLL
CCSCRYPT.DLL
Configuration
CCSCRYPT.DLL
CCSDRIVER.SYS
Configuration

FIGURE 1

5. Security Relevant Data Items

This section specifies the 3eTI Crypto Client's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3eTI Crypto Client.

5.1. Cryptographic Keys and CSPs

The 3e Crypto Client contains the following security relevant data items:

Security Relevant Data Items	SRDI Description
AES or 3DES Static Key	Data encryption/decryption using an AES static key (128, 192, or 256-bits) or 3DES static key (192-bits)
AES or 3DES Dynamic Broadcast Key	Data encryption/decryption using a dynamically exchanged AES key (128, 192, or 256-bits) or 3DES (192-bits)
AES or 3DES Dynamic Unicast Key	Data encryption/decryption using a dynamically exchanged AES key (128, 192, or 256-bits) or 3DES (192-bits)
AES system config key	A 128-bit key used to encrypt static keys and passwords stored in registry
HMAC SHA-1 Key	Key used to verify software integrity during power-up and integrity of RSA key files during dynamic key exchange
RSA Certificate	Sent to Security Server during EAP-TLS negotiation
RSA Private Key	Used to sign messages during EAP-TLS
TDES Key	Password-derived key used to encrypt private key file (not considered encrypted for FIPS purposes)
Crypto-officer password	CO Password
Administrator password	Administrator Password

5.2. Access Control Policy

The 3eTI Crypto Client maintains and enforces the access control policy for each SRDI stored within the module. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read (R), write (W), execute (E). If no permission is listed, then the operator cannot access the SRDI. The following table defines the access that an operator has to each SRDI and through which services.

3e Crypto Client SRDI Roles and Services Access Policy	Security Relevant Data Item	AES or TDES Static Key	AES or TDES Dynamic Broadcast	AES or TDES Dynamic Unicast	AES system config key	HMAC SHA-1 Key	RSA Certificate	RSA Private Key	TDES Key	CO Password	Administrator Password
Role/Service											
Crypto-officer Role											
Client Encryption settings		W	E	E	E	E	R/E	R/E	E		
Client Configuration											
Client status						E					
User Login					E					E	
User Password Change					E					W	
Administrator Role											
Client Encryption settings											
Client Configuration											
Client status						E					
User Login					E						E
User Password Change					E						W
Gateway Role											
Sending/Receiving data		E	W/E	E			E				
Security Server Role											
Provides authentication				R			E				

6. Mitigation of other attacks

The module does not provide mitigation against any commonly known attacks. FIPS 140-2 Level 2 does not require a specific security policy for mitigation of other attacks except those for which testable requirements are defined in the standard.